Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for securing management frames, the method comprising the steps of:

establishing an authenticated relationship between a transmitter and a receiver on a network;

generating a client-specific management frame protection key;

deriving an information element based upon the client-specific management frame protection key for signing a management frame packet transmitted on the network;

embedding the information element into the management frame packet;

transmitting the management frame packet to the receiver;

receiving the management frame packet; and

validating the information element in the received management frame packet.

2. (Original) The method set forth in claim 1 wherein the information element includes a message integrity check information element.

3. (Original) The method set forth in claim 1 further comprising the steps of:

generating a replay protection value for signing the management frame packet; and

adding the replay protection value into the management frame packet prior to transmitting.

4. (Original) The method set forth in claim 3 further comprising the step of validating the replay protection value.

5. (Original) The method set forth in claim 1 wherein the step of generating a key is concurrent with the step of establishing an authenticated relationship.

6. (Original) The method set forth in claim 1 wherein the step of establishing an authenticated relationship further includes employing a key establishment protocol.

7. (Original) The method set forth in claim 1 wherein the step of validating the information element further comprises the step of comparing the information element with a locally derived information element established by the receiver.

8. (Original) The method set forth in claim 2 wherein the step of validating the information element further comprises the step of comparing the message integrity check information element of the received management frame packet with a locally derived message integrity check information element established by the receiver.

9. (Original) The method set forth in claim 3 wherein the step of validating the information element further comprises the step of comparing the replay protection value of the received management frame packet with a locally derived replay protection value established by the receiver.

10. (Original) The method set forth in claim 1 wherein the receiver includes an access point.

11. (Original) The method set forth in claim 1 wherein the transmitter includes a wireless client.

12. (Original) The method set forth in claim 2 further comprising the step of generating the message integrity check value for the management frame packet prior to transmitting.

13. (Currently Amended) A system for securing a management frame packet, the system comprising:

means for authenticating a relationship between a transmitter and a receiver;

means for generating a client-specific management frame protection key;

means for deriving ~~generating~~ an information element based upon the client-specific management frame protection key for signing the management frame packet transmitted between the transmitter and the receiver via a network;

means for adding the information element into the management frame packet;

means for transmitting the management frame packet to the receiver via the network;

means for receiving the management frame packet; and

means for validating the information element in the received management frame packet.

14. (Original) The system set forth in claim 13 wherein the information element includes a message integrity check information element.

15. (Original) The system set forth in claim 14 wherein the information element further includes a replay protection value.

16. (Original) The system set forth in claim 13 wherein the means for transmitting the management frame packet is an IEEE 802.11 protocol.

17. (Cancelled)

18. (Original) The method set forth in claim 14, wherein the message integrity check information element uniquely identifies the management frame communication to the authenticator.

19. (Currently Amended) A method for preventing IEEE 802.11 session disruption on a network, comprising the steps of:

establishing a communication link between an access point and a wireless client on the network;

creating a trust relationship between the access point and the wireless client such that the wireless client is adapted to securely access the network;

establishing a client-specific key for signing a management frame packet configured to be transmitted between the access point and the wireless client;

generating a message integrity check value based upon the client-specific key;

calculating a replay protection value for signing the management frame packet;

embedding the message integrity check value and the replay protection value into ~~a header of~~ the management frame packet;

transmitting the management frame packet comprising the message integrity check value and the replay protection value ~~header~~ to the access point; and

authenticating the message integrity check value and the replay protection value~~header~~.

Claims 20-21 (Cancelled)

22. (Original) The method set forth in claim 19 wherein the step of authenticating further comprises the steps of:

calculating a local replay protection value;

generating a local message integrity check value;

comparing the received replay protection value with the local replay protection value; and

comparing the received message integrity check value with the local message integrity check value.

Claims 23-27 (Cancelled)